ArmorPoint MDR

Statement of Work

Contents

ArmorPoint MDR Service Scope

ARMORPOINT PLATFORM AND TECHNOLOGY

ENDPOINT DETECTION AND RESPONSE AGENTS

ArmorPoint will provide EDR software agents to Client for install on in-scope Endpoints and Servers that are on supported operating systems. The EDR agents will provide the following functions and services:

- Anti-Virus
- Anti-Malware
- Exploit Protection
- PowerShell and .Net Protection
- Anti-Ransomware

LOG COLLECTION AND RETENTION

The ArmorPoint log retention policy is as follows unless otherwise specified in Order Form:

- Security Alerts / Incidents / Vulnerabilities / Tickets
    - 365 Days Online and Searchable
- Benign Data (Anything not related to Alerts, Incidents, Vulnerabilities, Tickets)
    - Examples include unrelated Windows Event, Network Device and/or Agent Performance logs, etc.
    - 30 Days Online and Searchable
    - 365 Days Archived and Retrievable

SOC DASHBOARD AND LOG ANALYTICS

ArmorPoint will provide a SOC Dashboard for correlation and reporting of collected data and events.

ARMORPOINT SECURITY OPERATIONS CENTER (SOC)

MANAGEMENT SERVICES

ArmorPoint will provide SOC Platform management services which includes:

- Platform Health, Security, and Maintenance
- Platform Support
    - User Training as requested
    - Standard Dashboard and Report Configuration

- Alert Rule Generation
- Event-Handling

MONITORING

ArmorPoint will provide 24x7x365 monitoring of Alerts and Incidents (definitions below) within the SOC Platform. This will include:

- Alert assignment and management of all generated and open alerts
- Initial alert investigation to determine if any suspicious behavior is occurring
- Upon alert investigation, ArmorPoint will action the alert, which may include any of the following:
  - Closing the alert with the following documentation inside the platform:
    - Resolution Type
    - Resolution Synopsis
    - Resolution Actions
    - Resolution Notes
  - Engage and notify Client via pre-built notification policies with investigation notes and confirmation of activity
    - Client is responsible for responding to that engagement with direction on how to proceed
  - Escalate the alert into an Incident to be worked by the ArmorPoint Incident Management Team and notify Client via pre-built notification policies of such escalation
- Incident escalation, assignment and management of all escalated and created Incidents

1.1.1 Alert Definition

An Alert is an observable, measurable anomalous occurrence in a system or network. An example of an alert is an instance of unsuccessful logon, system crash, unplanned reboot, degradation in service performance, or network traffic spike. Alerts are monitored, reviewed, and analyzed by the ArmorPoint SOC Team and either confirmed to be benign or escalated to the level of an Incident.

1.1.2 Incident Definition

An Incident is an observable, measurable event taking place in a system or network that deviates from the normal behavior and implies harm or threat to do harm. Additionally, an event involving accidental loss of sensitive information is also classified as an Incident. An example of an Incident would be any unauthorized access and/or disclosure of confidential information, successful or repeated network intrusion attempt, or detection of any unwanted / malicious application or process. Upon confirmation of an Incident, ArmorPoint Incident Response services are invoked.

MONITORING AND REMEDIATION PROCESS

ArmorPoint maintains a Security Incident Response Plan (IRP) that will be reviewed and tested annually. Appropriate training will be provided to any staff with responsibilities as part of the Security Incident Response Team (IRT).

ArmorPoint's SOC bases its IRP on the SANS Institute's Incident Handling methodology. The SANS Incident Handling methodology divides the response process into six phases: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. The basic premise of this methodology is that organizations are constantly in a state of Incident response and are responsible for performing actions based on the phase they are in; the default phase is Preparation.

The Incident response process is determined by the severity level of the Incident. As the impact of an Incident becomes more significant or wide spread, the escalation level increases, bringing more resources to assist in addressing the Incident. At each escalation level, individuals who will be needed at the next higher level of escalation are alerted to the Incident so they will be ready to respond when they are needed. The ArmorPoint SOC maintains 24x7 availability of IT individuals with additional on-call support as required for Incident response and monitoring coverage for any evidence of unauthorized activity, unauthorized system use, and alerts.

1.1.3 Preparation

The Preparation phase for an Incident takes place before the Incident is identified and establishes the capability to identify Security Incidents in a timely manner and provide guidance to minimize damage from identified Incidents.

The ArmorPoint SOC IRT is authorized to leverage all necessary equipment, communication methods, offices, conference rooms, and other ArmorPoint resources for handling an Incident. This includes contacting all available on-call support personnel.

1.1.4 Identification

The objective of the Identification phase is to determine if a Security Incident has occurred and determine its severity based on the impact and scope of the Incident.

The ArmorPoint SOC Team is responsible for the monitoring of events and identification of suspicious activity on information systems and networks. The SOC monitors events and alerts from provided security tools and notifies the Client in the event that suspicious activity is identified as per established Service Level Agreements (SLA's) corresponding to determined event criticality.

All Security Incidents / notifications are documented and tracked within the ArmorPoint platform.

Where communication is required, the SOC will reference an Incident Response Plan (IRP) contact list provided by the Client to ensure the appropriate individual or group is getting the appropriate level of communication.

If it is suspected that the email system has been compromised, this communication will not take place via email unless email encryption not controlled by the email server is used. Alternatively, other secure communication methods may be utilized.

1.1.5 Containment

The objective of the Containment phase is to mitigate risk of additional exposure or damage from a Security Incident. Containment efforts may include actions such as quarantining systems, terminating processes, and/or blocking network traffic at the endpoint level, if technically available. All Incident response activities must be carried out in a manner which does not further jeopardize the confidentiality, availability, or integrity of systems and information.

The ArmorPoint SOC Team will provide all available information, to include containment recommendations, to the Client's designated support team prior to implementing changes. In the event containment services are initiated, specific containment steps are at the discretion / approval of the Client.

1.1.6 Guided Eradication

The objective of the Eradication phase is to directly address the Security Incident and eliminate the root cause. Eradication efforts may include actions such as ArmorPoint quarantining processes or files or devices, guidance around uninstalling software, or consulting on creating/modifying firewall rules.

The ArmorPoint SOC Team will provide all available information, to include eradication recommendations, to the Client's designated support team prior to implementing changes. In the event containment services are initiated, specific eradication steps are at the discretion / approval of the Client.

1.1.6.1 Post-Eradication Scope

Once the threat has been confirmed as being contained and is no longer active, ArmorPoint MDR includes **five (5)** "use it or lose it" hours per month of the following services. Any hours above the use of originating five (5) hours, will be billed at $300.00/Hour:

1.1.7 Recovery

The objective of the Recovery phase is to resume normal operations and return any compromised systems, applications, and devices into production. After the system has been returned to production, its operation must be monitored to ensure the compromise does not recur and the system(s) are operating properly. Required steps during recovery could include unblocking an IP address, allowing or exempting processes / applications from being blocked.

1.1.8 Lessons Learned

The objective of the Lessons Learned phase is to identify root causes of the Incident and develop a plan for preventing similar Incidents from occurring in the future.

The ArmorPoint team will provide documentation of all Incident Response activity within the ArmorPoint portal. Reporting will include information on how the incident was identified, the impact of the incident, any persons notified of the incident, and steps taken to remediate the incident. Client follow-up will be initiated before incident closure.

Closing meetings should occur no later than two weeks after completion of the Recovery phase. This meeting should review the incident report and is an opportunity to reflect on the incident response process to identify opportunities for improvement.

DISCLAIMER

By accepting this agreement, the Client understands that the below items are the responsibility of the Client to implement and maintain. In the event that these best practices are not initiated, Client understands that they are operating in a non-supported manner, and ArmorPoint is not responsible for any performance impacts or security incidents that may occur:

- Set EDR agent in prevention mode with appropriate modules, not detection mode
- ArmorPoint is not responsible for security incidents originating from unmonitored devices.
- System Requirements are as follows, if system requirements are unable to be met, alternative agentless approach will be discussed with client. (Additional fees may apply)
    - Machine RAM: 4GB
    - CPU: Dual Core 2GHZ Core I3 and above or equivalent
    - Available Disk Space: 1.5 GB Minimum
    - Network Connectivity: Ethernet or Wi-Fi

MULTIPLE EDR RISK ACCEPTANCE AGREEMENT

The Parties agree to the following relating to operating multiple “EDR” (Endpoint Detection and Response) or “MDR” (Managed Detection and Response) or “AV” (Anti-Virus) Tools.

ArmorPoint’s solution includes its own EDR tool that can be run in conjunction with a previously installed EDR, MDR or AV tool.

ArmorPoint recommends all clients to singularly use the EDR tool provided as part of the ArmorPoint solution and discontinue use of multiple EDR, MDR or AV tools as part of their security stack.

With this understanding, Client accepts this risk if dual EDRs are in use and acknowledges the following:

- Client is choosing to run multiple EDR, MDR or AV tools in their current deployment.
- Client acknowledges that running multiple EDR, MDR or AV tools can cause the following challenges:
    - Resource consumption issues on the device with multiple tools.
    - There is risk that the competing tools could interfere with each other's processes.
    - Client is responsible for setting exceptions and assigning policies to allow the ArmorPoint EDR tool to operate and ensure there are no conflicts.
    - There are scenarios where one tool may interfere with collection of data and block files, giving off illusion one tool did not block against it, when the competing tool never had the opportunity to assess the data as potentially malicious.
    - Having two security products running simultaneously can cause unexpected behavior

Client hereby acknowledges ArmorPoint SOC team will work on best effort to support client environment, but may be hindered by a lack of visibility due to multiple tools being operated.

END OF LIFE DEVICE AND OPERATING SYSTEM RISK ACCEPTANCE AGREEMENT

The Parties agree to the following relating to End of Life Devices and Operating Systems (Appendix A):

- ArmorPoint does not provide SIEM agent installers for end of life devices and/or operating systems.
- ArmorPoint recommends all clients upgrade to supported versions as soon as possible.
- End of life devices and/or operating systems are unable to continue to be patched from a security perspective and are high risk security profiles for both client and ArmorPoint to support.

With this understanding, Client accepts this risk and acknowledges the following:

- ArmorPoint does not provide installers or collectors for device logs to be collected by the SIEM;
- ArmorPoint will provide EDR agent to devices where an EDR package has an approved installer on specific end of life devices;
- If the EDR agent does not install properly on an end of life device, troubleshooting becomes responsibility of the Client;
- ArmorPoint will provide an EDR agent and installer, but there is no guarantee on performance or protection of those devices;
- Any such non-supported devices are not included in the bucket of support hours provided by ArmorPoint; and,
- Any remediation work specifically tied to end of life devices and/or operating systems will be billed at $300.00 / hour by Trapp

**End of Life Devices and/or Operating Systems are defined as any device or operating system that has ended or limited support on the product and/or version from originating manufacturer or software company for maintenance purposes (software updates and security patches) and/or troubleshooting. See Appendix A for current list of in-scope Operating Systems.*

CLIENT ENVIRONMENT FAILURES

Client agrees that ArmorPoint will not be liable for any failure to provide the SOC Services if such failure is caused by Client's failure to meet the applicable requirements for each Service. At a minimum, Client is responsible for ensuring the following environmental failures do not negatively impact the Services:

Service interruptions or degradations due to any Client supplied internet or private access whether provided by Client or third parties engaged by Client or equipment when provided by Client or third parties engaged by Client.

Failure or deficient performance of Client-supplied power, equipment, services, or systems.

Client's failure to adhere to SOC recommended configurations on managed or unmanaged equipment that affects the Service.

Failure to provide a secure environment for on-premise devices, including, but not limited to secure mounting/racking, appropriate cooling and air handling, secure from theft, etc.

Service interruptions or degradations in Service caused by a piece of equipment, configuration, routing event or technology required to be operative in order to perform that is under the management and control of Client.

Contractual Changes

This SOW may change and ArmorPoint may update this SOW from time to time. It is your responsibility to check this SOW periodically for changes.

The following Governance structure defines the Contract Change Process:

Change To	Vehicle	Process
Service scope	Change of scope presented with justification and supporting data. Changes that cause a change to the monthly cost to Client of more than $1,000 will require further Executive Approval through a Contract Change process.	Order Form
New project or effort	Each proposed effort or initiative will be presented to executive leadership and/or board with supporting charter, solution outline and estimates.	Order Form
Change to the overall service requirements and performances	Each change will be presented to the Executive and be processed with further Executive Approval	Contract CCR or Addendum
Change to the scope, terms and conditions of the current	Each change will be presented to the Executive and be processed with further Executive Approval	Contract Addendum

Exclusions

The following exclusions apply to the scope of the work stated above and have been incorporated into the pricing stated below:

- Implementation of technology, including software agents, is not included within the Statement of Work
- Any work or services not expressly provided for herein
- Any application development or integration efforts not expressly provided for herein
- Any actual hardware purchases for on-premise needs
- Any migration or upgrade of Client infrastructure (servers, network, etc.)
- Any actual implementation of the recommendations made by ArmorPoint unless specified in this document
- Any efforts tied to re-installing OS due to virus or malware or any system instability after the removal of a virus
- Any work related to being crypto-locked. ArmorPoint will work to mitigate the spread by blocking at the edge and/or taking machines offline
- Any data recovery and forensics work due to purposeful or malicious Client or application errors
- Any software license or physical hardware expenses
- Any software license that's not explicitly mentioned, and not covered by ArmorPoint
- All Travel and lodging costs
- Any fees related to shipping, handling, customs, duties and/or taxes
- Any additional work requested beyond the scope of this Agreement will be expressly set forth by subsequent agreement, including, but not limited to, a Contract Change Request ("CCR")

Service Level Targets

The following constitutes the reference for performance and expectations regarding this entire agreement. Updates to the Service Level Targets will automatically become enforced upon their execution or approval by both Client and ArmorPoint unless specified otherwise.

HOURS OF OPERATION - 24X7X365 SUPPORT

SERVICE GUIDELINES

The ArmorPoint Service Desk uses a Triaged Response Metrics system to prioritize Client Alerts or Incidents. The below Triaged Response Metrics outlines our standard service level commitments for communicating the Alert or Incident status to Client.

TICKET PRIORITY DEFINITIONS

Priority of a ticket is defined by its impact and urgency. Impact and urgency are determined according to the chart below and assigned by ArmorPoint:

	Urgency		
Impact	**Tertiary System**	**Secondary System**	**Core Business Service**
All users	High	High	Critical
Group of users	Medium	High	Critical
One User	Low	Medium	High

RESPONSE TARGET METRICS FOR ALERTS & INCIDENTS

ArmorPoint's definition of a "response" is the time it has taken a SOC analyst to start an investigation after an alert or incident has been created.

Priority	Response Target
High or Critical Priority	30 Minutes
Medium Priority	2 Hours
Low Priority	4 Hours

RESOLUTION TARGET METRICS

Resolution targets are best effort with priority given based on severity.

Revision History

Document Version	Published Date	Description or Notes
5.1	11/30/2022	Added Disclaimers for Multiple EDR, EOL Risk Acceptance and Client Environment Failure
5.2	12/05/2023	Added various clarifications around service; Added Monitoring definitions